



Brenda Sprague

May 5, 2009

Senate Committee on the Judiciary
Subcommittee on Terrorism and Homeland Security
Field Hearing
"The Passport Issuance Process: Closing the Door to Fraud"
Dirksen Senate Office Building
Room 226
Washington, D.C.
May 5, 2009
2:30 p.m.

Testimony of
Deputy Assistant Secretary of State for Consular Affairs
Brenda S. Sprague

Chairman Cardin, Senator Kyl, Senator Feinstein, and distinguished members of the Subcommittee,

I appreciate this opportunity to discuss the passport issuance process and the plans we have to address our fraud vulnerabilities. We take seriously our responsibility to protect U.S. borders and the integrity of the U.S. passport through vigilant adjudication. The Bureau of Consular Affairs (CA) works diligently to improve training, procedures, and oversight throughout the passport adjudication process. The outcome of the General Accountability Office's (GAO) recent investigation shows that we need to do more. We have already taken a number of immediate actions, and are in the process of devising a detailed plan to enhance our entire process and program.

As you already have been briefed, a GAO investigative team informed CA on February 10, 2009, that they had performed a probe of the passport issuance process. The team reported that a GAO investigator submitted four passport applications (three at local postal acceptance facilities and one at a passport agency) utilizing a combination of counterfeit or fraudulently obtained documents. All four applications resulted in U.S. passports being issued in error. The subsequent GAO report specifically identified two major/significant vulnerabilities in our process: one, that Passport Specialists were unknowingly approving applications before all information checks were completed; and two, Passport Specialists and acceptance agents did not recognize fraudulent documents.

CA immediately initiated a number of measures to address these vulnerabilities and to mitigate potential fraud in the future. Some measures taken or contemplated would be more appropriately discussed only in a closed session.

First, upon receiving information from the GAO regarding the four passports issued in error, we promptly identified each passport, and, in accordance with standard operating procedures, we revoked the passports and posted corresponding "lookout alerts" in our internal systems and with U.S. border officials and Interpol.

We suspended adjudication approval authority for the four Passport Specialists who issued the four GAO applications.

We suspended the authority of the acceptance facilities that accepted the three GAO applications.

We immediately provided counterfeit document detection refresher training to all passport agency managers and specialists. Bi-weekly "case study" meetings are being held by agency/center supervisors with the Passport Specialists regarding unfamiliar or fraudulent documentation received in the office. The GAO report was shared with passport agency staff to reiterate the importance of carefully reviewing identification and citizenship documents, as well as the information on passport applications, to detect fraud. In addition, we revised performance standards for Passport Specialists to re-emphasize the importance of quality adjudication and fraud prevention performance standards.

We instituted a 100 percent audit of all live applications. Passport Specialists were released from the audit only when they had demonstrated to their supervisors that they were processing work in full compliance with adjudication standards as related to both proper annotation and attention to possible fraud indicators.

We revised our procedures regarding the processing of same day "Will Call" service and routine cases. Additional supervisory oversight is required for all same day "Will Call" applications. Agencies/centers have been directed to complete all information checks prior to the issuance of the passport. These procedural changes enhance our ability to identify potential fraudulent applications or documents. Additionally, passport acceptance agents at post offices and courthouses, and Passport Specialists at our passport agency public counters, must now photocopy all identification documentation submitted by applicants so it can become part of the permanent passport application record.

Second, we created an Adjudication Policy and Process Review Working Group in mid-March to help further identify necessary improvements. This Working Group consists of five subgroups, which are:

- Restructuring of Adjudication Process and Oversight – This subgroup is reviewing the current adjudication program and working on recommendations to restructure our processes. Additionally, the subgroup is working on recommendations for a new adjudicative managerial oversight program.
- Adjudication Requirements and Standards – This subgroup is developing standardized desk and counter adjudication procedures. Additionally, it is developing standardized procedures for Passport Specialists regarding the use of the Social Security Number (SSN) and other commercial databases.
- Post-Issuance Audit – This subgroup is developing a statistically valid audit process for previously issued passports. The results from this audit will be used for future training purposes.
- Training Initiatives – This subgroup is identifying enhancements for fraud training for all Passport Specialists, Supervisors, and Fraud Prevention Managers (FPMs). It is reviewing the curriculum of the National Training Program (NTP), which we use for training our new employees, to ensure that it appropriately and thoroughly addresses the document verification requirements used by Passport Specialists. Also, the subgroup is identifying and recommending standard requirements for on-the-job training for new hires once they complete NTP and begin working with "live" (unapproved) applications. Additionally, it is developing standardized fraud awareness training for our courthouse and post office acceptance facilities.
- Technology – This subgroup is identifying technical and procedural vulnerabilities to the integrity of the passport process. Additionally, it is working on recommendations for improvement to our automated systems through access to additional databases.

Formal recommendations from the subgroups are expected by summer 2009. Shortly afterward, they will be compiled, finalized, and forwarded for Department management approval.

Third, CA is already working on some long-term initiatives to address our process vulnerabilities. We are currently pursuing an initiative to combine the systems platforms for domestic and overseas passport adjudication and issuance to ensure consistency and improve overall quality control. The combined system will utilize as many automated adjudication checks as possible.

The GAO Report recommended that we work with state level officials to develop a strategy to gain access to their databases and incorporate reviews of these databases into our adjudication process. Prior to the GAO undercover test, CA officials had held ongoing meetings with federal and state government agencies regarding access to information and databases for citizenship and identity verification. As a result of the GAO's recent recommendation, I also sent a letter to all State Registrars asking for their assistance in providing the Department access to their birth and death records for verification purposes. We plan to vigorously continue this effort.

I appreciate the opportunity to share with you the Department of State's comprehensive approach to enhancing U.S. border security by augmenting the security of all aspects of the U.S. passport program. We appreciate GAO's constructive recommendations and look forward to working with Congress and the GAO to produce the most secure passport possible. Let me end by assuring you that the Department is fully committed to a secure passport issuance process, and deterring and detecting fraud.

Mr. Chairman, thank you again for the opportunity to be here today. I will be pleased to answer any questions that you, the Ranking Member, and the other distinguished members of the Subcommittee might have.

[Privacy and Security Information](#)